

Amendments to the Claims

1 Claim 1 (currently amended): A computer program product for enabling a subsequent user sign-  
2 on during a certificate-based host access session, said computer program product embodied on a  
3 computer-readable medium and comprising:

4 computer-readable program code means for processing a first sign-on during a secure  
5 session using a digital certificate, further comprising:

6 computer-readable program code means for establishing said secure session from a  
7 client machine to a server machine using said digital certificate, wherein said digital certificate  
8 represents an identity of said client machine or a user thereof;

9 computer-readable program code means for storing said digital certificate or a  
10 reference thereto at said server machine;

11 computer-readable program code means for establishing a session from said server  
12 machine to a host system using a legacy host communication protocol, responsive to receiving, at  
13 said server machine, a first sign-on request from said client machine, wherein said first sign-on  
14 request identifies a first secure legacy host application to which said first sign-on is requested;

15 computer-readable program code means for passing said stored digital certificate  
16 or said reference from said server machine to a host access security system;

17 computer-readable program code means, operable in said host access security  
18 system, for authenticating said identity using said passed digital certificate or a retrieved  
19 certificate which is retrieved using said reference;

20 computer-readable program code means, operable in said host access security  
21 system, for using said passed or retrieved digital certificate to locate access credentials for said

Serial No. 09/619,205

-7-

Docket RSW9-2000-0035-US1

22 user;

23 computer-readable program code means, operable in said host access security  
24 system, for accessing a stored password or generating a password substitute representing said  
25 located credentials;

26 computer-readable program code means, operable in said host access security  
27 system, for returning said stored password or generated password substitute to said server  
28 machine, along with a first user identifier corresponding to said located credentials; and

29 computer-readable program code means, operable in said server machine, for using  
30 said returned stored password or said generated password substitute and said returned first user  
31 identifier to transparently complete said first sign-on, on behalf of said user of said client machine,  
32 to [[a]] said first secure legacy host application executing at said host system; and

33 computer-readable program code means for processing a subsequent sign-on of said user  
34 during said secure session using said digital certificate, wherein said subsequent sign-on requests  
35 access to said secure legacy host application or a different legacy host application; further  
36 comprising:

37 computer-readable program code means for receiving a subsequent sign-on  
38 request, at said server machine from said client machine, wherein: (1) said subsequent sign-on  
39 request identifies a second secure legacy host application to which said subsequent sign-on is  
40 requested; (2) said subsequent sign-on requires authenticating a requester of said subsequent sign-  
41 on requiring said identity; (3) said second secure legacy host application may be identical to said  
42 first secure legacy host application; and (4) said requester of said subsequent sign-on is said user;

43 computer-readable program code means, operable at said server machine, for

44 retrieving said stored digital certificate or reference;

45 computer-readable program code means for passing said retrieved digital  
46 certificate or reference from said server machine to said host access security system;

47 computer-readable program code means, operable in said host access security  
48 system, for re-authenticating said identity of said user, thereby authenticating said requester, using  
49 said passed retrieved digital certificate or retrieved reference;

50 computer-readable program code means, operable in said host access security  
51 system, for using said passed retrieved digital certificate or retrieved reference to again re-locate  
52 said access credentials for said user;

53 computer-readable program code means, operable in said host access security  
54 system, for re-accessing said stored password or generating a new password substitute  
55 representing said re-located credentials;

56 computer-readable program code means, operable in said host access security  
57 system, for returning said re-accessed stored password or generated new password substitute to  
58 said server machine, along with said user identifier corresponding to said re-located credentials;  
59 and

60 computer-readable program code means, operable in said server machine, for using  
61 said returned re-accessed stored password or [[said]] new password substitute and said returned  
62 user identifier corresponding to said re-located credentials to transparently complete said  
63 subsequent sign-on, on behalf of said requester, to said second secure legacy host application  
64 executing at said host system or ~~said different legacy host application.~~

1 Claim 2 (currently amended): The computer program product as claimed in Claim 1, wherein said  
2 digital certificate ~~[[is an]]~~ and said second digital certificate are X.509 certificate certificates and  
3 said digital certificate reference is a reference to an X.509 certificate.

1 Claim 3 (original): The computer program product as claimed in Claim 1, wherein said  
2 communication protocol is a 3270 emulation protocol.

1 Claim 4 (original): The computer program product as claimed in Claim 1, wherein said  
2 communication protocol is a 5250 emulation protocol.

a7  
1 Claim 5 (original): The computer program product as claimed in Claim 1, wherein said  
2 communication protocol is a Virtual Terminal protocol.

1 Claim 6 (original): The computer program product as claimed in Claim 3, wherein said host  
2 access security system is a Resource Access Control Facility (RACF) system.

1 Claim 7 (original): The computer program product as claimed in Claim 1, wherein said server  
2 machine is a Web application server machine.

1 Claim 8 (currently amended): The computer program product as claimed in Claim 1, wherein:  
2 said computer-readable program code means for processing said first sign-on further  
3 comprising comprises:

Serial No. 09/619,205

-10-

Docket RSW9-2000-0035-US1

\_\_\_\_\_ computer-readable program code means for requesting by said first secure legacy host application, responsive to said computer-readable program code means for establishing said session, first sign-on information for said user; and

\_\_\_\_\_ computer-readable program code means for responding to said request for first sign-on information by sending a first sign-on message with placeholders from said client machine to said server machine, said placeholders representing a user identification and a password of said user; and

said computer-readable program code means for using said returned password or password substitute and said returned first user identifier to transparently complete said first sign-on further comprises:

\_\_\_\_\_ computer-readable program code means for substituting [[a]] said returned user identifier ~~associated with said located access credentials~~ and said returned stored password or said generated password substitute for said placeholders in said first sign-on message, thereby creating a revised first sign-on message; and

computer-readable program code means for forwarding said revised first sign-on message from said server machine to said first secure legacy host application.

~~\_\_\_\_\_ computer-readable program code means for requesting, by said legacy host application, subsequent sign-on information for said user;~~

~~\_\_\_\_\_ computer-readable program code means for responding to said request for subsequent sign-on information by sending a subsequent sign-on message with placeholders from said client machine to said server machine, said placeholders representing said user identification and said password of said user; and~~

Serial No. 09/619,205

-11-

Docket RSW9-2000-0035-US1

26 ~~\_\_\_\_\_ computer-readable program code means for substituting said user identifier associated~~  
27 ~~with said re-located access credentials and said re-accessed stored password or said new~~  
28 ~~password substitute for said placeholders in said subsequent sign-on message.~~

1 Claim 9 (currently amended): The computer program product as claimed in Claim 7, wherein:  
2 said computer-readable program code means for using said returned password or  
3 password substitute and said returned first user identifier to transparently complete said first sign-  
4 on further comprising comprises:

5 \_\_\_\_\_ computer-readable program code means for requesting by said first secure legacy  
6 host application, responsive to said computer-readable program code means for establishing said  
7 session, first sign-on information for said user; and

8 \_\_\_\_\_ computer-readable program code means for responding to said request for first  
9 sign-on information by supplying from said server machine to said first secure legacy host  
10 application, [[a]] said returned user identifier associated with said located access credentials and  
11 said returned stored password or said generated password substitute at said server machine;

12 \_\_\_\_\_ computer-readable program code means for requesting, by said legacy host application,  
13 subsequent sign-on information for said user; and

14 \_\_\_\_\_ computer-readable program code means for responding to said request for subsequent  
15 sign-on information by supplying said user identifier associated with said re-located access  
16 credentials and said re-accessed stored password or said new password substitute at said server  
17 machine.

1 Claim 10 (currently amended): A system for enabling a subsequent user sign-on during a  
2 certificate-based host access session, comprising:

3 means for processing a first sign-on during a secure session using a digital certificate,  
4 further comprising:

5 means for establishing said secure session from a client machine to a server  
6 machine using said digital certificate, wherein said digital certificate represents an identity of said  
7 client machine or a user thereof;

8 means for storing said digital certificate or a reference thereto at said server  
9 machine;

10 means for establishing a session from said server machine to a host system using a  
11 legacy host communication protocol, responsive to receiving, at said server machine, a first sign-  
12 on request from said client machine, wherein said first sign-on request identifies a first secure  
13 legacy host application to which said first sign-on is requested;

14 means for passing said stored digital certificate or said reference from said server  
15 machine to a host access security system;

16 means, operable in said host access security system, for authenticating said identity  
17 using said passed digital certificate or a retrieved certificate which is retrieved using said  
18 reference;

19 means, operable in said host access security system, for using said passed or  
20 retrieved digital certificate to locate access credentials for said user;

21 means, operable in said host access security system, for accessing a stored  
22 password or generating a password substitute representing said located credentials;

Serial No. 09/619,205

-13-

Docket RSW9-2000-0035-US1

23 means, operable in said host access security system, for returning said stored password or  
24 generated password substitute to said server machine, along with a first user identifier  
25 corresponding to said located credentials; and

26 means, operable in said server machine, for using said returned stored password or  
27 said-generated password substitute and said returned first user identifier to transparently complete  
28 said first sign-on, on behalf of said user of said client machine, to [[a]] said first secure legacy host  
29 application executing at said host system; and

30 means for processing a subsequent sign-on of said user during said secure session using  
31 said digital certificate, wherein said subsequent sign-on requests access to said secure legacy host  
32 application or a different legacy host application; further comprising:

a 33 means for receiving a subsequent sign-on request, at said server machine from said  
34 client machine, wherein: (1) said subsequent sign-on request identifies a second secure legacy  
35 host application to which said subsequent sign-on is requested; (2) said subsequent sign-on  
36 requires authenticating a requester of said subsequent sign-on requiring said identity; (3) said  
37 second secure legacy host application may be identical to said first secure legacy host application;  
38 and (4) said requester of said subsequent sign-on is said user;

39 means, operable at said server machine, for retrieving said stored digital certificate  
40 or reference;

41 means for passing said retrieved digital certificate or reference from said server  
42 machine to said host access security system;

43 means, operable in said host access security system, for re-authenticating said  
44 identity of said user, thereby authenticating said requester, using said passed retrieved digital

Serial No. 09/619,205

-14-

Docket RSW9-2000-0035-US1



45 certificate or retrieved reference;

46 means, operable in said host access security system, for using said passed retrieved  
47 digital certificate or retrieved reference to again re-locate said access credentials for said user;

48 means, operable in said host access security system for re-accessing said stored  
49 password or generating a new password substitute representing said re-located credentials;

50 means, operable in said host access security system for returning said re-accessed  
51 stored password or generated new password substitute to said server machine, along with said  
52 user identifier corresponding to said re-located credentials; and

53 means, operable in said server machine, for using said returned re-accessed stored  
a 54 password or [[said]] new password substitute and said returned user identifier corresponding to  
55 said re-located credentials to transparently complete said subsequent sign-on, on behalf of said  
56 requester, to said second secure legacy host application executing at said host system or said  
57 different legacy host application.

1 Claim 11 (currently amended): The system as claimed in Claim 10, wherein said digital certificate  
2 [[is an]] and said second digital certificate are X.509 certificate certificates and said digital  
3 certificate reference is a reference to an X.509 certificate.

1 Claim 12 (original): The system as claimed in Claim 10, wherein said communication protocol is  
2 a 3270 emulation protocol.

1 Claim 13 (original): The system as claimed in Claim 12, wherein said host access security system

Serial No. 09/619,205

-15-

Docket RSW9-2000-0035-US1

is a Resource Access Control Facility (RACF) system.

Claim 14 (original): The system as claimed in Claim 10, wherein said server machine is a Web application server machine.

Claim 15 (currently amended): The system as claimed in Claim 10, wherein:

said means for processing said first sign-on further comprising comprises:

\_\_\_\_\_ means for requesting by said first secure legacy host application, responsive to said means for establishing said session, first sign-on information for said user; and

\_\_\_\_\_ means for responding to said request for first sign-on information by sending a first sign-on message with placeholders from said client machine to said server machine, said placeholders representing a user identification and a password of said user; and

said means for using said returned password or password substitute and said returned first user identifier to transparently complete said first sign-on further comprises:

\_\_\_\_\_ means for substituting [[a]] said returned user identifier ~~associated with said located access credentials~~ and said returned stored password or ~~said generated~~ password substitute for said placeholders in said first sign-on message, thereby creating a revised first sign-on message; and

means for forwarding said revised first sign-on message from said server machine to said first secure legacy host application.

\_\_\_\_\_ ~~means for requesting, by said legacy host application, subsequent sign-on information for said user;~~

Serial No. 09/619,205

-16-

Docket RSW9-2000-0035-US1

18 ~~\_\_\_\_\_ means for responding to said request for subsequent sign-on information by sending a~~  
19 ~~subsequent sign-on message with placeholders from said client machine to said server machine;~~  
20 ~~said placeholders representing said user identification and said password of said user; and~~  
21 ~~\_\_\_\_\_ means for substituting said user identifier associated with said re-located access credentials~~  
22 ~~and said re-accessed stored password or said new password substitute for said placeholders in~~  
23 ~~said subsequent sign-on message.~~

1 Claim 16 (currently amended): The system as claimed in Claim 14, wherein:

2 said means for using said returned password or password substitute and said returned first  
3 user identifier to transparently complete said first sign-on further comprising comprises:

4 \_\_\_\_\_ means for requesting by said first secure legacy host application, responsive to said  
5 means for establishing said session, first sign-on information for said user; and

6 \_\_\_\_\_ means for responding to said request for first sign-on information by supplying,  
7 from said server machine to said first secure legacy host application, [[a]] said returned user  
8 identifier associated with said located access credentials and said returned stored password or said  
9 generated password substitute at said server machine;

10 \_\_\_\_\_ means for requesting, by said legacy host application, subsequent sign-on information for  
11 said user; and

12 \_\_\_\_\_ means for responding to said request for subsequent sign-on information by supplying said  
13 user identifier associated with said re-located access credentials and said re-accessed stored  
14 password or said new password substitute at said server machine.

Serial No. 09/619,205

-17-

Docket RSW9-2000-0035-US1

1 Claim 17 (currently amended): A method for enabling a subsequent user sign-on during a  
2 certificate-based host access session, comprising the steps of:

3 processing a first sign-on during a secure session using a digital certificate, further  
4 comprising the steps of:

5 establishing said secure session from a client machine to a server machine using  
6 said digital certificate, wherein said digital certificate represents an identity of said client machine  
7 or a user thereof;

8 storing said digital certificate or a reference thereto at said server machine;

9 establishing a session from said server machine to a host system using a legacy  
10 host communication protocol, responsive to receiving, at said server machine, a first sign-on  
11 request from said client machine, wherein said first sign-on request identifies a first secure legacy  
12 host application to which said first sign-on is requested;

13 passing said stored digital certificate or said reference from said server machine to  
14 a host access security system;

15 authenticating, by said host access security system, said identity using said passed  
16 digital certificate or a retrieved certificate which is retrieved using said reference;

17 using, by said host access security system, said passed or retrieved digital  
18 certificate to locate access credentials for said user;

19 accessing, by said host access security system, a stored password or generating a  
20 password substitute representing said located credentials;

21 returning, by said host access security system, said stored password or generated  
22 password substitute to said server machine, along with a first user identifier corresponding to said

Serial No. 09/619,205

-18-

Docket RSW9-2000-0035-US1

23 located credentials; and

24 using, by said server machine, said returned stored password or said-generated  
25 password substitute and said returned first user identifier to transparently complete said first sign-  
26 on, on behalf of said user of said client machine, to [[a]] said first secure legacy host application  
27 executing at said host system; and

28 processing a subsequent sign-on of said user during said secure session using said digital  
29 certificate, wherein said subsequent sign-on requests access to said secure legacy host application  
30 or a different legacy host application; further comprising the steps of:

31 receiving a subsequent sign-on request, at said server machine from said client  
32 machine, wherein: (1) said subsequent sign-on request identifies a second secure legacy host  
33 application to which said subsequent sign-on is requested; (2) said subsequent sign-on requires  
34 authenticating a requester of said subsequent sign-on requiring said identity; (3) said second  
35 secure legacy host application may be identical to said first secure legacy host application; and (4)  
36 said requester of said subsequent sign-on is said user;

37 retrieving, by said server machine, said stored digital certificate or reference;  
38 passing said retrieved digital certificate or reference from said server machine to  
39 said host access security system;

40 re-authenticating, by said host access security system, said identity of said user,  
41 thereby authenticating said requester, using said passed retrieved digital certificate or retrieved  
42 reference;

43 using, by said host access security system, said passed retrieved digital certificate  
44 or retrieved reference to again re-locate said access credentials for said user;

Serial No. 09/619,205

-19-

Docket RSW9-2000-0035-US1

45 re-accessing, by said host access security system, said stored password or  
46 generating a new password substitute representing said re-located credentials;  
47 returning, by said host access security system, said re-accessed stored password or  
48 generated new password substitute to said server machine, along with said user identifier  
49 corresponding to said re-located credentials; and  
50 using, by said server machine, said returned re-accessed stored password or  
51 [[said]] new password substitute and said returned user identifier corresponding to said re-located  
52 credentials to transparently complete said subsequent sign-on, on behalf of said requester, to said  
53 second secure legacy host application executing at said host system or said different legacy host  
54 application.

a7

1 Claim 18 (currently amended): The method as claimed in Claim 17, wherein said digital  
2 certificate [[is an]] and said second digital certificate are X.509 certificate certificates and said  
3 digital certificate reference is a reference to an X.509 certificate.

1 Claim 19 (original): The method as claimed in Claim 17, wherein said communication protocol is  
2 a 3270 emulation protocol.

1 Claim 20 (original): The method as claimed in Claim 19, wherein said host access security system  
2 is a Resource Access Control Facility (RACF) system.

1 Claim 21 (original): The method as claimed in Claim 17, wherein said server machine is a Web

Serial No. 09/619,205

-20-

Docket RSW9-2000-0035-US1

2 application server machine.

1 Claim 22 (currently amended): The method as claimed in Claim 17, wherein:

2 said step of processing said first sign-on further comprising comprises the steps of:

3 \_\_\_\_\_ requesting by said first secure legacy host application, responsive to said step of  
4 establishing said session, first sign-on information for said user; and

5 \_\_\_\_\_ responding to said request for first sign-on information by sending a first sign-on  
6 message with placeholders from said client machine to said server machine, said placeholders  
7 representing a user identification and a password of said user; and

8 said step of using said returned password or password substitute and said returned first  
9 user identifier to transparently complete said first sign-on further comprises the steps of:

10 \_\_\_\_\_ substituting [[a]] said returned user identifier associated with said located access  
11 credentials and said returned stored password or said generated password substitute for said  
12 placeholders in said first sign-on message, thereby creating a revised first sign-on message; and

13 forwarding said revised first sign-on message from said server machine to said first  
14 secure legacy host application.

15 ~~\_\_\_\_\_ requesting, by said legacy host application, subsequent sign-on information for said user;~~

16 ~~\_\_\_\_\_ responding to said request for subsequent sign-on information by sending a subsequent~~  
17 ~~sign-on message with placeholders from said client machine to said server machine, said~~

18 ~~placeholders representing said user identification and said password of said user; and~~

19 ~~\_\_\_\_\_ substituting said user identifier associated with said re-located access credentials and said~~  
20 ~~re-accessed stored password or said new password substitute for said placeholders in said~~

Serial No. 09/619,205

-21-

Docket RSW9-2000-0035-US1

21 ~~subsequent sign-on message.~~

1 Claim 23 (currently amended): The method as claimed in Claim 21, wherein:

2 said step of using said returned password or password substitute and said returned first  
3 user identifier to transparently complete said first sign-on further comprising comprises the steps  
4 of:

5 \_\_\_\_\_ requesting by said first secure legacy host application, responsive to said step of  
6 establishing said session, first sign-on information for said user; and

7 \_\_\_\_\_ responding to said request for first sign-on information by supplying, from said  
8 server machine to said first secure legacy host application, [[a]] said returned user identifier

9 ~~associated with said located access credentials and said returned stored password or said~~  
10 ~~generated password substitute at said server machine;~~

11 ~~\_\_\_\_\_ requesting, by said legacy host application, subsequent sign-on information for said user;~~  
12 ~~and~~

13 ~~\_\_\_\_\_ responding to said request for subsequent sign-on information by supplying said user~~  
14 ~~identifier associated with said re-located access credentials and said re-accessed stored password~~  
15 ~~or said new password substitute at said server machine.~~

1 Claim 24 (new): The computer program product as claimed in Claim 1, wherein:

2 said computer-readable program code means for processing said subsequent sign-on  
3 further comprises:

4 computer-readable program code means for requesting, by said second secure

Serial No. 09/619,205

-22-

Docket RSW9-2000-0035-US1



5 legacy host application, subsequent sign-on information for said requester; and

6 computer-readable program code means for responding to said request for  
7 subsequent sign-on information by sending a subsequent sign-on message with placeholders from  
8 said client machine to said server machine, said placeholders representing said user identification  
9 and said password of said user; and

10 said computer-readable program code means for using said returned re-accessed password  
11 or new password substitute and said returned user identifier corresponding to said re-located  
12 credentials to transparently complete said second sign-on further comprises:

13 computer-readable program code means for substituting said returned user  
14 identifier corresponding to said re-located credentials and said returned re-accessed password or  
15 new password substitute for said placeholders in said subsequent sign-on message, thereby  
16 creating a revised subsequent sign-on message; and

17 computer-readable program code means for forwarding said revised subsequent  
18 sign-on message from said server machine to said second secure legacy host application.

1 Claim 25 (new): The computer program product as claimed in Claim 7, wherein said computer-  
2 readable program code means for processing said subsequent sign-on further comprises:

3 computer-readable program code means for requesting, by said second secure legacy host  
4 application, subsequent sign-on information for said requester; and

5 computer-readable program code means for responding to said request for subsequent  
6 sign-on information by supplying, from said server machine to said second secure legacy host  
7 application, said returned user identifier associated with said re-located credentials and said

Serial No. 09/619,205

-23-

Docket RSW9-2000-0035-US1

8 returned re-accessed password or new password substitute.

1 Claim 26 (new): The system as claimed in Claim 10, wherein:

2 said means for processing said subsequent sign-on further comprises:

3 means for requesting, by said second secure legacy host application, subsequent  
4 sign-on information for said requester; and

5 means for responding to said request for subsequent sign-on information by  
6 sending a subsequent sign-on message with placeholders from said client machine to said server  
7 machine, said placeholders representing said user identification and said password of said user;  
8 and

a7 9 said means for using said returned re-accessed password or new password substitute and  
10 said returned user identifier corresponding to said re-located credentials to transparently complete  
11 said second sign-on further comprises:

12 means for substituting said returned user identifier corresponding to said re-located  
13 credentials and said returned re-accessed password or new password substitute for said  
14 placeholders in said subsequent sign-on message, thereby creating a revised subsequent sign-on  
15 message; and

16 means for forwarding said revised subsequent sign-on message from said server  
17 machine to said second sure legacy host application.

1 Claim 27 (new): The system as claimed in Claim 14, wherein said means for processing said  
2 subsequent sign-on further comprises:

Serial No. 09/619,205

-24-

Docket RSW9-2000-0035-US1

3 means for requesting, by said second secure legacy host application, subsequent sign-on  
4 information for said requester; and

5 means for responding to said request for subsequent sign-on information by supplying,  
6 from said server machine to said second secure legacy host application, said returned user  
7 identifier associated with said re-located credentials and said returned re-accessed password or  
8 new password substitute.

1 Claim 28 (new): The method as claimed in Claim 17, wherein:

2 said step of processing said subsequent sign-on further comprises the steps of:

3 requesting, by said second secure legacy host application, subsequent sign-on  
4 information for said requester; and

a<sup>n</sup> 5 responding to said request for subsequent sign-on information by sending a  
6 subsequent sign-on message with placeholders from said client machine to said server machine,  
7 said placeholders representing said user identification and said password of said user; and

8 said step of using said returned re-accessed password or new password substitute and said  
9 returned user identifier corresponding to said re-located credentials to transparently complete said  
10 second sign-on further comprises the steps of:

11 substituting said returned user identifier corresponding to said re-located  
12 credentials and said returned re-accessed password or new password substitute for said  
13 placeholders in said subsequent sign-on message, thereby creating a revised subsequent sign-on  
14 message; and

15 forwarding said revised subsequent sign-on message from said server machine to

Serial No. 09/619,205

-25-

Docket RSW9-2000-0035-US1

16 said second secure legacy host application.

1 Claim 29 (new): The method as claimed in Claim 21, wherein said step of processing said  
2 subsequent sign-on further comprises the steps of:

3 requesting, by said second secure legacy host application, subsequent sign-on information  
4 for said requester; and

5 responding to said request for subsequent sign-on information by supplying, from said  
6 server machine to said second secure legacy host application, said returned user identifier  
7 associated with said re-located credentials and said returned re-accessed password or new  
8 password substitute.

27

1 Claim 30 (new): A computer-implemented method for enabling an identity to be subsequently  
2 provided during a certificate-based host access session, comprising steps of:

3 establishing a secure session between a client and a server using a digital certificate owned  
4 by a user of said client;

5 remembering said digital certificate at said server;

6 completing a first sign-on to a host application, by said server on behalf of said user,  
7 responsive to receiving an asynchronous sign-on request from said client that identifies said host  
8 application, further comprising the steps of:

9 using said remembered digital certificate to authenticate said user to a host access  
10 security component;

11 if said user is authenticated, locating, by said host access security component,

Serial No. 09/619,205

-26-

Docket RSW9-2000-0035-US1

12 access credentials of said user;  
13 creating, by said host access security component, a passticket that represents said  
14 located access credentials;  
15 returning said passticket from said host access security component to said server,  
16 along with a user identifier associated with said located access credentials; and  
17 inserting, by said server, said passticket and said user identifier into a log-on  
18 message in place of placeholders therefor, when said log-on message is received at said server  
19 from said client, thereby creating a revised log-on message that is then sent from said server to  
20 sign said user on to said host application; and  
21 completing a subsequent sign-on to a second host application, by said server on behalf of  
22 said user, responsive to receiving a second asynchronous sign-on request from said client that  
23 identifies said second host application, wherein said second host application may be identical to  
24 said host application, further comprising the steps of:  
25 passing said remembered digital certificate from said server to said host access  
26 security component for authenticating said user for access to said second host application;  
27 if said user is authenticated for access to said second host application, locating, by  
28 said host access security component, second access credentials of said user, wherein said second  
29 access credentials may be identical to said located access credentials;  
30 creating, by said host access security component, a second passticket that  
31 represents said located second access credentials of said user;  
32 returning said second passticket from said host access security component to said  
33 server, along with a second user identifier associated with said second located access credentials;

Serial No. 09/619,205

-27-

Docket RSW9-2000-0035-US1

34 and

35 inserting said returned second passticket and said returned second user identifier

a<sup>7</sup> 36 into a subsequent log-on message that is then sent from said server to sign said user on to said

37 second host application.

---